⧈ PitneyBowes

RECEIVED
CENTRAL FAX CENTER

OCT 2 4 2005

Pitney Bowes Inc.

Assistant Deputy General
Corporate Counsel,
Intellectual Property &
Technology Law
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

203-924-3880
203-924-3919 Fax
Steve.shapiro@pb.com
www.pitneybowes.com

Facsimile

To: Patent and Trademark Office
        Attention: Examiner Firmin Backer, Group Art Unit: 3621
Facsimile No.:   1-703-872-9306
From: Steven J. Shapiro
Date: October 24, 2005
Subject: Serial No.: 09/474,326
Pages: 13 (including this cover)

Re: U.S. Patent Application Serial No.: 09/474,326
Confirmation No. 3621
Our Docket No. E-977

Enclosed please find a Brief on Appeal in the above referenced application.
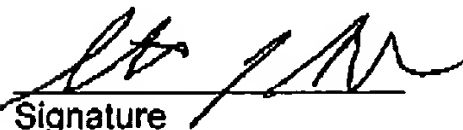
CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that the following correspondence is being transmitted
Via Facsimile to:

        Patent and Trademark Office
        Attention: Examiner Firmin Backer, Group Art Unit: 3621
        Facsimile No.   1-703-872-9306

October 24, 2005
Date of Transmission

Steven J. Shapiro
Name of Registered Rep.

Signature

October 24, 2005
Date

{00042302.1 }

RECEIVED
CENTRAL FAX CENTER

OCT 24 2005

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF APPEALS AND PATENT INTERFERENCES

In re patent application of:	) Date: October 24, 2005
Thomas J. Foth et al.	) Attorney Docket No.: E-977
Serial No.: 09/474,326	) Customer No.:00919
Filed: December 29, 1999	) Group Art Unit: 3621
Confirmation No.: 2120	) Examiner: Firmin Backer

Title: METHOD FOR FACILITATING A TRANSACTION BETWEEN A
MERCHANT AND A BUYER

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is being filed pursuamt to 35 U.S.C. Section 134 from the final rejection of claims 1-8 mailed May 25, 2005. **Pursuant to MPEP 1208.02, no fee is believed due because the fee for filing this Brief on Appeal was previously paid for in this application with the filing of a prior Brief on Appeal**. However, if fees for this appeal are deemed to be required, authorization is hereby given to charge such fees to deposit account number 16-1885.

REAL PARTY IN INTEREST

The real party in interest is Pitney Bowes Inc. which acquired all rights to the above-identified application by way of an assignment which was recorded in

{I0042239.1 }

PAGE 2/13 * RCVD AT 10/24/2005 10:56:04 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/0 * DNIS:8729306 * CSID:203 924 3919 * DURATION (mm-ss):03-16

- 2 -

the Assignment Branch of the United States Patent and Trademark Office on December 29, 1999 at Reel 010484 and Frame 0726.

RELATED APPEALS AND INTERFERENCES

There are no related Appeals or Interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the instant appeal.

STATUS OF CLAIMS

The instant application was originally filed with claims 1-8. In the Amendment filed on July 15, 2002, claims 1, 2 ,4 and 7 were amended. No further Amendment to the claims was made. Accordingly, claims 1-8 are currently pending and are being appealed.

STATUS OF AMENDMENTS

No Amendments are currently pending. Pending claims 1-8 are set forth in Appendix A.

SUMMARY OF CLAIMED SUBJECT MATTER

Referring to Figures 1 and 2 and page 8 line 26 to page 10 line 21, the invention of **independent claim 1** is generally directed to a method for facilitating a transaction between a merchant **106** and a buyer **102**. The facilitation occurs through the use of a digital content file **180** that includes a header **202** with information (price, product ID, merchant ID, etc.) related to the purchasing of a digital content product (article, music, picture, etc.) and a digital content product in encoded form **206**. The digital content file **180** is downloaded into a computer **122** in a manner in which the header **202** is downloaded and at least some of the purchasing information is displayed at the computer **122** while the encoded digital content product **206** is concurrently being downloaded into the computer **122**. This concurrent operation improves the efficiency of the download since a buyer can be viewing the purchasing information to determine if a purchase will be made

{20042239.1 }

- 3 -

while the encoded digital content product **206** is being downloaded. Therefore, if a very large encoded digital product needs to be downloaded, this occurs in the background as the viewing and purchasing decision is being made. Accordingly, if a purchase is then requested, the encoded digital content file **206** is either completely downloaded and ready for decoding or at least a significant portion of it has been downloaded

The invention of **independent claim 4** is directed to a method that would allow, for example, a third party **118**, via a computer **132**, to access a web site **181** of a merchant **106** to encrypt digital content files at the merchant web site **181**. As set forth in dependent claims, the computer **132** is provided with the identification of the merchant's files that require encryption together with the web site location of the files and information as to how to access those files. The computer **132** connects to the web site **181**, such as through the Internet, and accesses, and encrypts the designated files and stores the encrypted files at the web site **181**. This permits remote encrypting of files at a merchant web site. (Figure 2 and page 20 line 4 to page 21 line 12).

As for **independent claim 7**, it is directed to a method whereby encrypted and unencrypted digital content product files are stored at a first computer, such as a merchant computer **126**. Upon request for the encrypted files they are sent to a second computer **122**. However, in the case of the unencrypted digital content product files they are dynamically encrypted prior to being sent to the second computer **122**. This method of distributing digital content using static encrypting and dynamic encrypting is discussed in detail on page 16 lines 3-25 of the specification with reference to Figures 1 and 2. The specification describes the benefits of this hybrid encrypting of files. That is, static encoding is efficient for content that is not subject to change (such as a particular piece of music) because time is saved if real time encryption is not required. However, constantly changing information, such as stock data, would require large amounts of continuous maintenance to store in encrypted form. Thus, for constantly changing data,

- 4 -

dynamic encryption is best suited since the downloaded product is encrypted real time for each product.

Independent claim 8 implements the steps of claim 1 on a computer **122.** Thus, the description of claim 1 set forth above is applicable to claim 8.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

At issue in this Appeal is the propriety of the following rejection:

1. Claims 1-8 stand rejected under 35 U.S.C. 102(e) as being anticipated by **Krishnan (U.S. Patent No. 6.073,124).**

ARGUMENTS

Claims 1,2,3 and 8

A rejection for anticipation under section 102 requires that each and every limitation of a claimed invention be disclosed in a single prior art reference. In re Paulsen, 30 F.3d1475, 1478-79, 31 USPQ2d 1671, 1673 (fed. Cir. 1994). For the reasons discussed below it is submitted that Krishnan fails to teach or suggest each and every limitation of claims 1,2,3, and 8.

The Examiner has cited Figure 2, the summary, Column 6 line 44 to column 7 line 43, and column 8 line 26 to column 10 line 55 of Krishnan for allegedly teaching each and every element of claims 1,2,3 and 8. However, Applicants submit that such is not the case. It is submitted that none of the aforementioned sections of Krishnan teach or suggest "the concurrent displaying of purchasing information with the downloading of encoded digital content" as set forth in claims 1 and 8.

Column 6 line 44 to column 7 line 43 of Krishnan describes a Secure Digital Commerce System (DCS) where, for example, a user via a web page 202 can select to purchase a digital content product ("Return of Arcade") by selecting icon 203 (Col. 6 line 44 to col. 7 line 5). Col. 7 lines 5 to 43 then describe that the DCS includes a DCS Server that downloads to a DCS Client an encrypted copy of the

- 5 -

selected digital content item and various components needed to license and purchase the merchandise and to unsecure (decrypt) and execute the licensed materials. There is simply no discussion in this referenced section of Krishnan of "the concurrent displaying of purchasing information with the downloading of encoded digital content" as set forth in claims 1 and 8 .

Column 8, line 26 to column 10 line 55 of Krishnan provides further details of the DCS but also does not teach or suggest the above recited limitation of claims 1 and 8. With reference to Figure 3 of Krishnan, the DCS client 301 includes a customer computer system 311 which interfaces with a virtual store 304 via a web browser application 303. The virtual store provides to the computer 311 download files 313 which each have a boot program and a component list. The boot program uses the component list to permit the computer 311 to obtain the secure digital content from the content supplier server 306 of the DCS Server 302. The download files (boot program and component lists) are stored in repository 305. The DCS server also includes a licensing and purchasing broker 307, a payment processing function 309, and a password generation repository, none of which relate to the digital content product except to the extent a licensing certificate is used to authorize use of the digital content product at the computer 311.

The summary of the invention in Krishnan, likewise does not teach or suggest the above recited limitation of claims 1 and 8. Accordingly, in view of the arguments set forth above it is submitted that claims 1, 2-3 (which depend from claim 1), and 8 are not anticipated by Krishnan.

Claims 4-6

Claim 4 provides the capability for a broker computer to encrypt files at a merchant computer. The broker computer is provided with an identification of the digital content files designated for encryption at a merchant's web site together with the web site location. Further, the broker computer is provided with information required to access the digital content files. Using the above

{X0042239.1 }

- 6 -

information the broker computer accesses and encrypts the digital content files at the merchant web site such that the digital content files are stored in encrypted form. Krishnan simply does not teach or suggest these limitations. In the Krishnan system, the client computer 311 uses the downloaded files 313 to identify the digital content product to the content supplier server 306, but there is no discussion of a broker computer identifying and encrypting files at the content server 306.

Claim 7

As discussed in the summary of the Claimed Subject Matter, claim 7 is directed to a method for distributing digital content products from a first computer to a second computer. The digital content files are either stored in encrypted or unencrypted form at the first computer. When encrypted files are requested by the second computer they are sent by the first computer. However, when unencrypted files are requested, they are dynamically encrypted and sent to the second computer. The use of the dynamic encryption is benefial for constantly changing data as it reduces the need for extensive maintenance that would be required to keep the constantly changing data stored in an encrypted form.
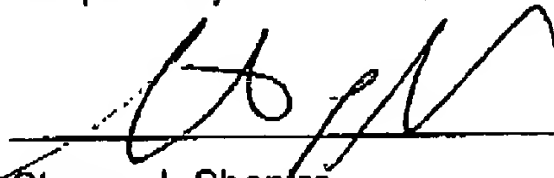
In Krishnan, the content server 306 stores secure digital content product and not both encrypted and unencrypted digital content product as set forth in claim 7. Further, Krishnan never discusses dynamically encrypting digital content product being sent from a first computer to a second computer as recited in claim 7. Krishnan only discusses the downloading of an encrypted digital content product. Krishnan does discuss at column 8 lines 55-58 that the download files 313 can be generated dynamically, but this is not the same as dynamically encrypting the digital content product. The download files 313 are not digital content product but are simply used to identify and download the digital content from the content supplier server 306. The actual digital content is stored at content server 306 in a secure manner and is not dynamically encrypted during its download to the customer system 311.

SUMMARY

It is submitted for each of the reasons enumerated above that claims 1-8 are not anticipated by or rendered obvious in view of the applied reference. Accordingly, the Appellants respectfully request that the Board reverse the Examiner with respect to the rejections set forth in the final Office Action.

Respectfully submitted,

Steven J. Shapiro
Reg. No. 35,677
Attorney of Record
Telephone (203) 924-3880

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that the following correspondence is being transmitted
Via Facsimile to:

Patent and Trademark Office
Attention: Examiner Firmin Backer, Group Art Unit: 3621
Facsimile No.   1-703-872-9306

October 24, 2005   Steven J. Shapiro
Date of Transmission   Name of Registered Rep.

Signature   October 24, 2005
                                          Date

{I0042239.1 }

- 8 -

APPENDIX A - Claims

1.   A method for using a computer to facilitate a transaction between a merchant and a buyer, the method comprising the steps of:

downloading into the computer a digital content file of the merchant, the digital content file including a header with information related to purchasing a digital content product and the digital content product in encoded form; and

using the computer for reading the downloaded header and displaying at least some of the information related to purchasing the digital content product while concurrently downloading the encoded digital content product into the computer.

2.   A method as recited in claim 1, further comprising inputting a request to purchase the digital content product into the computer, outputting from the computer the request to purchase to a broker computer, receiving at the computer from the broker computer a key for decoding the encoded digital content product in response to the request to purchase, and using the key at the computer to decode the encoded digital content product to create a decoded digital content product while concurrently displaying the decoded digital content product.

3.   A method as recited in claim 2, further comprising concurrently downloading the encoded digital content product into the computer while decoding the encoded digital content product and displaying the decoded digital content product.

4.   A method for using a computer by a broker to encrypt digital content product files of a merchant that are hosted at a merchant web site, the method comprising the steps of:

inputting into the computer an identification of the digital content product files designated for encryption together with the web site location of the digital

- 9 -

content product files and information required to access the digital content product files;

via the computer, connecting to the web site and accessing and encrypting the digital content product files designated for encryption; and

storing the encrypted digital content product files at the web site.

5.   A method as recited in claim 4, further comprising inputting into the computer a location at the web site where each of the encrypted digital content product files are to be stored, and storing the encrypted digital content product files at the location.

6.   A method as recited in claim 5, further comprising using the computer to create a buyer product file for each encrypted digital content product file, the buyer product file including the encrypted digital content product file and a header having information about the digital content product file for use by a buyer in making a decision on whether to purchase the digital content product.

7.   A method for distributing from a first computer digital content products for purchase, the method comprising the steps of:

encrypting a first digital content product file;

statically storing the encrypted first digital content product file at the first computer;

storing a second digital content product file in unencrypted form at the first computer; and

inputting a request into the first computer for downloading from the first computer to a second computer at least one of the encrypted first digital content product file and the second digital content product file;

wherein at times when the request is for the encrypted first digital content product file downloading the encrypted first digital content file to the second computer, and at times when the request is for the second digital content product file dynamically encrypting the second digital content product file and sending the

{20042339.1 }

PAGE 10/13 * RCVD AT 10/24/2005 10:56:04 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/0 * DNIS:8729306 * CSID:203 924 3919 * DURATION (mm-ss):03-16

- 10 -

second digital content product file in encrypted form to the second computer while maintaining the storing of the second digital content product file in unencrypted form at the first computer.

8.   A computer having a computer-readable medium including computer-executable instructions for performing the steps of receiving and storing in the computer a digital content file of a merchant, the digital content file including a header with information related to purchasing a digital content product and the digital content product in encoded form; and reading the stored header and displaying at least some of the information related to purchasing the digital content product while concurrently receiving the encoded digital content product into the computer.

- 11 -

APPENDIX B –Evidence

None

- 12 -

APPENDIX C –Related Proceedings

None

THIS PAGE BLANK (USPTO)